Exhibit A

COMPLAINT WITH JURY DEMAND

Exhibit A

COMJD
MARK J. BOURASSA, ESQ. (NBN 7999)
JENNIFER A. FORNETTI, ESQ. (NBN 7644)
VALERIE S. GRAY, ESQ. (NBN 14716)
THE BOURASSA LAW GROUP
2350 W. Charleston Blvd., Suite 100
Las Vegas, Nevada 89102
Telephone: (702) 851-2180
Facsimile: (702) 851-2189
Email: *mbourassa@blgwins.com*
jfornetti@blgwins.com
vgray@blgwins.com

GARY F. LYNCH (*pro hac vice* forthcoming)
NICHOLAS A. COLELLA (*pro hac vice* forthcoming)
PATRICK D. DONATHEN (*pro hac vice* forthcoming)
LYNCH CARPENTER LLP
1133 Penn Avenue, 5th Floor
Pittsburgh, Pennsylvania 15222
Telephone: (412) 322-9243
Email: *gary@lcllp.com*
nickc@lcllp.com
patrick@lcllp.com

Attorneys for Plaintiff

CASE NO: A-23-868157-C
Department 14

DISTRICT COURT
CLARK COUNTY, NEVADA
***

JENNIFER TAUSINGA, on behalf of herself and all others similarly situated; Plaintiff, vs. HANKINS & SOHN PLASTIC SURGERY ASSOCIATES, an unknown entity; HANKINS PLASTIC SURGERY ASSOCIATES, P.C., a domestic professional corporation; DOES 1 through 20, inclusive Defendants.	Case No.: Dept No.: **COMPLAINT AND DEMAND FOR JURY TRIAL**

COMPLAINT AND DEMAND FOR JURY TRIAL

Plaintiff JENNIFER TAUSINGA ("Plaintiff") by and through her attorneys of record, The Bourassa Law Group, hereby submits her Complaint against Defendants, and each of them, and alleges as follows:

I. INTRODUCTION

1. Healthcare providers that collect and store sensitive information about their patients have a duty to safeguard that information and ensure it remains private. This responsibility is essential where a Healthcare provider keeps and stores its patients' Personally Identifiable Information (or "PII") such as, *inter alia*, their first and last names, driver's license numbers, home addresses, telephone numbers, email addresses, and dates of birth.

2. This responsibility is also essential where a Healthcare provider keeps and stores its patients' personal health information (or "PHI") such as, *inter alia*, their medical history, medical consultation notes and photographs.

3. Plaintiff Tausinga brings this class action individually and on behalf of individuals that have had their sensitive PII/PHI disclosed and obtained by unknown third-parties as a result of Defendants' failure to properly secure and safeguard the PII/PHI described above.

4. On or about March 14, 2023, Defendants notified affected patients and/or prospective patients, including Plaintiff Tausinga of "a recent data security event that may impact some of your information. We are providing you with information about the event, our response, and steps you can take to better protect your information against the possibility of misuse of your information, should you feel it appropriate to do so. We recently became aware of allegations by an unknown actor that data was stolen from our network. We are working diligently to assess these allegations and to confirm the nature and scope of the activity. We are also actively working with law enforcement to investigate the activity. We are reviewing the information that we store on our systems to identify current and former patients whose information may have been impacted by this event. …" (the "Data Breach")

5. The Data Breach was a direct result of Defendants' failure to implement adequate and reasonable cyber-security procedures and protocols necessary to protect customer PII and/or PHI.

6. Defendants disregarded the rights of Plaintiff and Class Members (defined below) by, *inter alia*, intentionally, willfully, recklessly, or negligently failing to take adequate and reasonable measures to ensure its data systems were protected against unauthorized intrusions; failing to disclose that it did not have adequately robust computer systems and security practices to safeguard customer PII and/or PHI; failing to take standard and reasonably available steps to prevent the Data Breach; failing to monitor and timely detect the Data Breach; and failing to provide Plaintiff and Class Members prompt and accurate notice of the Data Breach.

7. As a result of Defendants' failure to implement and follow basic security procedures, Plaintiff's and Class Members' PII is now in the hands of cybercriminals.

8. Plaintiff and Class Members are now at a significantly increased and certainly impending risk of fraud, identity theft, and similar forms of criminal mischief, risk which may last for the rest of their lives. Consequently, Plaintiff and Class Members must devote substantially more time, money, and energy to protect themselves, to the extent possible, from these crimes.

9. Plaintiff, on behalf of all others similarly situated, alleges claims for negligence, breach of implied contract, unjust enrichment, breach of confidence and violation of the Nevada Consumer Fraud Act and seeks to compel Defendants to adopt reasonably sufficient security practices to safeguard customer PII that remains in its custody in order to prevent incidents like the Data Breach from reoccurring in the future.

II.
PARTIES

10. Plaintiff is and, at all times relevant hereto, was a resident of Clark County, Nevada.

11. Plaintiff is a patient of Defendants. She has provided her PII and PHI to Defendants in their normal course of business with the reasonable expectation that Defendants would safeguard her PII and keep her PHI confidential.

12. On or about March 14, 2023, Plaintiff received a notification from Defendants indicating that her PII and/or PHI may have been affected by the Data Breach.

13. Plaintiff suffered actual injury from having their PII and PHI stolen as a result of the Data Breach including, but not limited to: (a) paying monies to Defendants for its goods and services which she

would not have had if Defendants disclosed that it lacked data security practices adequate to safeguard consumers' PII/PHI from theft; (b) damages to and diminution in the value of their PII/PHI—a form of intangible property that Plaintiff entrusted to Defendants as a condition of receiving Defendants' services; (c) loss of their privacy; (d) imminent and impending injury arising from the increased risk of fraud and identity theft and further humiliation.

14. Defendant HANKINS & SOHN PLASTIC SURGERY ASSOCIATES (hereinafter "HSPS"), is, and at all times relevant hereto, was an unknown entity who is licensed to and is conducting business in Clark County, Nevada.

15. Defendant HANKINS PLASTIC SURGERY ASSOCIATES, P.C. (hereinafter "HSPA"), is, and at all times relevant hereto, was a professional corporation who is licensed to and is conducting business in Clark County, Nevada.

16. At all relevant times, DOES 1 through 20 inclusive, and each of them, were legal entities or individuals doing business in the State of Nevada. That the true names and capacities, whether individual, corporate, agents, association or otherwise of DOES 1 through 20, inclusive, are unknown to Plaintiff, who therefore sues said Defendants by such fictitious names. Plaintiff is informed and believes, and thereon alleges, that each of the DOE Defendants designated herein as DOES are responsible in some manner for the events and happenings herein referred to, and in some manner proximately caused the injuries and damages thereby to Plaintiff, as herein alleged. Plaintiff will ask leave of Court to amend the Complaint to insert the true names and capacities of the DOE Defendants and state appropriate charging allegations when that information has been ascertained.

17. DOES 1 through 8 are employers of Defendants who may be liable for Defendants' negligence pursuant to NRS §41.130. As of the filing of this Complaint, Plaintiff is not sure as to the identity of the proper entities or whether they are individuals, partnerships, limited partnerships, corporations, association of individuals in business, or some other form of business ownership, and as soon as the exact nature of the individuals or entities are known, Plaintiff will amend this Complaint and will substitute the exact names of the proper defendant in place of DOES 1 through 8.

18. DOES 9 through 20 may be individuals or entities who were responsible for the Data Breach and/or in some other way responsible for Plaintiff's damages. As of the filing of this Complaint,

Plaintiff is not sure as to the identity of the proper entities or whether they are individuals, partnerships, limited partnerships, corporations, association of individuals in business, or some other form of business ownership, and as soon as the exact nature of the individuals or entities are known, Plaintiff will amend this Complaint and will substitute the exact names of the proper defendant in place of DOES 9 through 20.

19. At all times hereinafter, HSPS, HSPA, and DOES 1 through 20 will be collectively referred to as Defendants.

20. At all times hereinafter, each Defendant was the joint venturer, principal, agent and/or employee of each of the other Defendants, and in doing the things herein described was acting jointly with consent, and within the course and scope as such joint venture, principal, agent and/or employee.

III.
JURISDICTION AND VENUE

21. This Court has jurisdiction in this matter, and venue is proper, in that all the facts and circumstances that give rise to the subject lawsuit occurred in Clark County, Nevada. Additionally, HSPS and HSPA reside in Clark County, Nevada.

IV.
GENERAL ALLEGATIONS

22. According to Defendants, they are "Las Vegas Plastic Surgeons providing their Plastic Surgery patients with the very best of surgical and nonsurgical care." https://www.hankinsplasticsurgery.com/ (last accessed March 30, 2023).

23. "At Hankins & Sohn Plastic Surgery Associates, our board certified plastic surgeons, W. Tracy Hankins, MD and Samuel M. Sohn, MD believe in patient safety, world-class results, and compassionate care. With this commitment in mind, we invite patients from around the world to experience the art and science of plastic surgery through the hands, hearts, and minds of Dr. Hankins and Dr. Sohn." https://www.hankinsplasticsurgery.com/about/ (last accessed March 30, 2023).

24. Plaintiff is informed and believes that Defendants collect, store, and maintain its patients' PII and PHI in the course of providing healthcare services.

///

25. In order to receive healthcare services offered by Defendants, patients must entrust their PII and/or PHI to Defendants, and in return, they reasonably expect that Defendants will safeguard their highly sensitive PII and/or PHI.

26. However, while Defendants "believe in patient safety," Defendants nevertheless employed inadequate data security measures to protect and secure the PII and/or PHI of patients entrusted to it, resulting in the Data Breach and compromise of Plaintiff's and Class members' PII and/or PHI.

A. The Value of Private Information and Effects of Unauthorized Disclosure.

27. Defendants were well aware that the PII and/or PHI they collect is highly sensitive and of significant value to those who would use it for wrongful purposes.

28. Defendants also knew that a breach of their computer systems, and exposure of the PII and/or PHI stored therein, would result in the increased risk of identity theft and fraud against the individuals whose PII/PHI was compromised.

29. These risks are not theoretical; in recent years, numerous high-profile breaches have occurred at business such as Equifax, Facebook, Yahoo, Marriott, Anthem, and many others.

30. PII/PHI has considerable value and constitutes an enticing and well-known target to hackers. Hackers easily can sell stolen data as there has been "proliferation of open and anonymous cybercrime forums on the Dark Web that serve as a bustling marketplace for such commerce."[1]

31. As the FTC recognizes, identity thieves can use this information to commit an array of crimes including identity theft, and medical and financial fraud.[2]

32. The prevalence of data breaches and identity theft has increased dramatically in recent years, accompanied by a parallel and growing economic drain on individuals, businesses, and government entities in the U.S. In 2021, there were 4,145 publicly disclosed data breaches, exposing 22 billion records. The United States specifically saw a 10% increase in the total number of data breaches.[3]

///

---

[1] Brian Krebs, The Value of a Hacked Company, Krebs on Security (July 14, 2016), http://krebsonsecurity.com/2016/07/the-value-of-a-hacked-company/.
[2] https://www.consumer.ftc.gov/articles/0271-warning-signs-identity-theft
[3] Data Breach Report: 2021 Year End, Risk Based Security (Feb. 4, 2022), https://www.riskbasedsecurity.com/2022/02/04/data-breach-report-2021-year-end/.

33. In tandem with the increase in data breaches, the rate of identity theft complaints has also increased over the past few years. For instance, in 2017, 2.9 million people reported some form of identity fraud compared to 5.7 million people in 2021.[4]

34. The healthcare industry has become a prime target for threat actors: "High demand for patient information and often-outdated systems are among the nine reasons healthcare is now the biggest target for online attacks."[5]

35. Additionally, "[h]ospitals store an incredible amount of patient data. Confidential data that's worth a lot of money to hackers who can sell it on easily – making the industry a growing target."[6]

36. Indeed, cybercriminals seek out PHI at a greater rate than other sources of personal information. In a 2022 report, the healthcare compliance company Protenus found that there were 905 medical data breaches in 2021, leaving over 50 million patient records exposed for 700 of the 2021 incidents. This is an increase from the 758 medical data breaches that Protenus compiled in 2020.[7]

37. The healthcare sector suffered about 337 breaches in the first half of 2022 alone, according to Fortified Health Security's mid-year report released in July. The percentage of healthcare breaches attributed to malicious activity rose more than 5 percentage points in the first six months of 2022 to account for nearly 80 percent of all reported incidents.[8]

38. The ramifications of Defendants' failure to keep Plaintiff and Class Members' PII and PHI secure are long lasting and severe. Once PII and PHI is stolen, fraudulent use of that information and damage to victims may continue for years. According to the U.S. Government Accountability Office, which conducted a study regarding data breaches, "in some cases, stolen data may be held for up to a year

---

[4] Insurance Information Institute, Facts + Statistics: Identity theft and cybercrime, Insurance Information Institute, https://www.iii.org/fact-statistic/facts-statistics-identity-theft-andcybercrime#Identity%20Theft%20And%20Fraud%20Reports,%202015-2019%20 (last visited Dec. 29, 2022).

[5] *The healthcare industry is at risk*, SwivelSecure https://swivelsecure.com/solutions/healthcare/healthcare-is-the-biggest-target-for-cyberattacks/ (last visited Mar. 28, 2023).

[6] *Id.*

[7] *2022 Breach Barometer*, PROTENUS, https://www.protenus.com/breach-barometer-report (last visited Mar. 28, 2023).

[8] Jill McKeon, *Health Sector Suffered 337 Healthcare Data Breaches in First Half of Year*, Cybersecurity News (July 19, 2022), available: https://healthitsecurity.com/news/health-sector-suffered-337-healthcare-data-breaches-in-first-half-of-year.

or more before being used to commit identity theft. Further, once stolen data have been sold or posted on the [Dark] Web, fraudulent use of that information may continue for years. As a result, studies that attempt to measure the harm resulting from data breaches cannot necessarily rule out all future harm."[9]

39. Even if stolen PII and PHI does not include financial or payment card account information, that does not mean there has been no harm, or that the breach does not cause a substantial risk of identity theft. Freshly stolen information can be used with success against victims in specifically targeted efforts to commit identity theft known as social engineering or spear phishing. In these forms of attack, the criminal uses the previously obtained PII about the individual, such as name, address, email address, and affiliations, to gain trust and increase the likelihood that a victim will be deceived into providing the criminal with additional information.

40. The breadth of data compromised in the Data Breach makes the information particularly valuable to thieves and leaves Defendants' patients especially vulnerable to identity theft, tax fraud, medical fraud, credit and bank fraud, and more.

41. Based on the value of its patients' PII and/or PHI to cybercriminals, Defendants knew or should have known, the importance of safeguarding the PII and/or PHI entrusted to it and of the foreseeable consequences if its data security systems were breached. Defendants failed, however, to take adequate cyber security measures to prevent the Data Breach from occurring.

B. Defendants Breached its Duty to Protect its Patients' PII and/or PHI.

42. Plaintiff is informed and believes that at some time before March 14, 2023, unauthorized individual(s) gained access to Defendants' patients' and potential patients' information systems and stole the PII and PHI of potentially hundreds of people, if not more.

43. On or about March 14, 2023, Defendants notified their patients' whose information was impacted by the Data Breach, including Plaintiff.

44. According to Defendants, the information obtained by the hackers could include the affected individuals' name, contact information, date of birth, Social Security number, driver's license information, medical history, consultation notes, and photographs.

---

[9] U.S. Gov't Accountability Office, Report to Congressional Requesters, Personal Information, June 2007: https://www.gao.gov/new.items/d07737.pdf (last visited Dec. 29, 2022).

45. Like Plaintiff, the Class Members received similar notices informing them that their PII and/or PHI was accessed and/or exfiltrated in the Data Breach.

46. Plaintiff is informed and believes that the Data Breach occurred as a direct result of Defendants' failure to implement and follow basic security procedures in order to protect its patients' PII and PHI.

47. By March 28, 2023, the hackers were threatening Plaintiff and Class Members through the WhatsApp mobile application to distribute the PII and PHI to Plaintiff's and Class members' friends, colleagues, and neighbors, unless they paid the hackers directly.

48. Plaintiff notified Defendants of the communication she received from the hackers.

49. When Plaintiff refused to pay the hackers' demands, the hackers shared her consultation photos with friends, colleagues, and neighbors. Defendants took no steps to prevent the release of the PII and/or PHI to Plaintiff's friends, colleagues, and neighbors. As a result of Defendants' failure to safeguard her PII and/or PHI, Plaintiff has been subjected to extortion and the mental anguish of having her sensitive PII and PHI exposed to her friends, colleagues, and neighbors.

C. FTC Guidelines Prohibit Defendants from Engaging in Unfair or Deceptive Acts or Practices.

50. Defendants are prohibited by the Federal Trade Commission Act, 15 U.S.C. § 45 ("FTC Act") from engaging in "unfair or deceptive acts or practices in or affecting commerce." The Federal Trade Commission ("FTC") has concluded that a company's failure to maintain reasonable and appropriate data security for consumers' sensitive personal information is an "unfair practice" in violation of the FTC Act.

51. The FTC has promulgated numerous guides for businesses that highlight the importance of implementing reasonable data security practices. According to the FTC, the need for data security should be factored into all business decision-making.[10]

52. The FTC provided cybersecurity guidelines for businesses, advising that businesses should protect personal customer information, properly dispose of personal information that is no longer needed,

[10] Start with Security – A Guide for Business, United States Federal Trade Comm'n (2015), https://www.ftc.gov/system/files/documents/plain-language/pdf0205-startwithsecurity.pdf.

encrypt information stored on networks, understand their network's vulnerabilities, and implement policies to correct any security problems.[11]

53. The FTC further recommends that companies not maintain PII longer than is needed for authorization of a transaction; limit access to private data; require complex passwords to be used on networks; use industry-tested methods for security; monitor for suspicious activity on the network; and verify that third-party service providers have implemented reasonable security measures.[12]

54. The FTC has brought enforcement actions against businesses for failing to adequately and reasonably protect customer data, treating the failure to employ reasonable and appropriate measures to protect against unauthorized access to confidential consumer data as an unfair act or practice prohibited by Section 5 of the FTC Act. Orders resulting from these actions further clarify the measures businesses must take to meet their data security obligations.

55. Defendants failed to properly implement basic data security practices. Defendants' failure to employ reasonable and appropriate measures to protect against unauthorized access to patients' PII and/or PHI constitutes an unfair act of practice prohibited by Section 5 of the FTC Act.

56. Defendants were at all times fully aware of its obligations to protect the PII and/or PHI of patients because of its position as a medical provider, which gave it direct access to reams of PII and/or PHI. Defendants were also aware of the significant repercussions that would result from its failure to do so.

D. Defendants are Obligated Under HIPAA to Safeguard Personal Information.

57. Defendants are required by the Health Insurance Portability and Accountability Act ("HIPAA"), 42 U.S.C. § 1302d, et seq. to safeguard patient PHI.

58. Defendants are entities covered by under HIPAA, which sets minimum federal standards for privacy and security of PHI.

///

///

---

[11] Protecting Personal Information: A Guide for Business, United States Federal Trade Comm'n, https://www.ftc.gov/system/files/documents/plain-language/pdf-0136_protetingpersonalinformationpdf

[12] *Id.*

59. HIPAA requires "compl[iance] with the applicable standards, implementation specifications, and requirements" of HIPAA "with respect to electronic protected health information." 45 C.F.R. § 164.302.

60. Under 45 C.F.R. § 160.103, HIPAA defines "protected health information" or PHI as "individually identifiable health information" that is "transmitted by electronic media; maintained in electronic media; or transmitted or maintained in any other form or medium."

61. Under C.F.R. 160.103, HIPAA defines "individually identifiable health information" as "a subset of health information, including demographic information collected from an individual" that is (1) "created or received by a health care provider;" (2)"[r]elates to the past, present, or future physical or mental health or condition of an individual; the provision of health care to an individual; or the past, present, or future payment for the provision of health care to an individual;" and (3) either (a) identifies the individual; or (b) with respect to which there is a reasonable basis to believe the information can be used to identify the individual."

62. HIPAA requires ILS to: (a) ensure the confidentiality, integrity, and availability of all electronic PHI it creates, receives, maintains, or transmits; (b) identify and protect against reasonably anticipated threats to the security or integrity of the electronic PHI; (c) protect against reasonably anticipated, impermissible uses, or disclosures of the PHI; and (d) ensure compliance by its workforce to satisfy HIPAA's security requirements. 45 CFR § 164.102, *et. seq*.

63. While HIPAA permits healthcare providers and their business associates to disclose PHI to third parties under certain circumstances, HIPAA does not permit healthcare providers and their business associates to disclose PHI to cybercriminals nor did Plaintiff or the Class Members consent to the disclosure of their PHI to cybercriminals.

64. As such, Defendants are required under HIPAA to maintain the strictest confidentiality of Plaintiff's and Class Members' PHI that they acquire, receive, and collect, and Defendants are further required to maintain sufficient safeguards to protect that information from being accessed by unauthorized third parties.

65. Given the application of HIPAA to Defendants, and that Plaintiff and Class Members directly or indirectly entrusted their PHI to Defendants in order to receive healthcare services from

Defendants, Plaintiff and Class Members reasonably expected that Defendants would safeguard their highly sensitive information and keep their PHI confidential.

E. Plaintiff and Class Members Suffered Damages.

66. The ramifications of Defendants' failure to keep PII/PHI secure are long lasting and severe. Once PII/PHI is stolen, fraudulent use of that information and damage to victims may continue for years.

67. Once PII/PHI is exposed, there is virtually no way to ensure that the exposed information has been fully recovered or obtained against future misuse. For this reason, Plaintiff and Class Members will need to maintain these heightened measures for years, and possibly their entire lives as a result of Defendants' conduct. Further, the value of Plaintiff and Class Members' PII and/or PHI has been diminished by its exposure in the Data Breach.

68. Plaintiff and Class Members are at substantial increased risk of suffering identity theft and fraud or misuse of their PII/PHI as a result of the Data Breach. From a recent study, 28% of consumers affected by a data breach become victims of identity fraud—this is a significant increase from a 2012 study that found only 9.5% of those affected by a breach would be subject to identity fraud. Without a data breach, the likelihood of identify fraud is only about 3%.[13]

69. Further, Plaintiff and Class Members have incurred and will incur out of pocket costs for protective measures, such as identity theft protection, credit monitoring, credit report fees, credit freeze fees, and similar costs related to the Data Breach.

70. Besides the monetary damage sustained in the event of identity theft, patients may have to spend hours trying to resolve identity theft issues. For example, the FTC estimates that it takes consumers an average of 200 hours of work over approximately six months to recover from identity theft.[14]

71. Plaintiff and Class Members are also at a continued risk because their information remains in Defendants' systems, which have already been shown to be susceptible to compromise and attack and

---

[13] Stu Sjouwerman, 28 Percent of Data Breaches Lead to Fraud, KnowBe4, https://blog.knowbe4.com/bid/252486/28-percent-of-data-breaches-lead-to-fraud (last visited Dec. 29, 2022).

[14] Kathryn Parkman, How to Report identity Theft, ConsumerAffairs (Feb. 17, 2022), https://www.consumeraffairs.com/finance/how-to-report-identity-theft.html.

is subject to further attack so long as Defendants fail to undertake the necessary and appropriate security and training measures to protect its patients' PII and/or PHI.

72. Plaintiff and Class Members have suffered emotional distress as a result of the Data Breach, the increased risk of identity theft and financial fraud, and the unauthorized exposure of their private information and/or photos to strangers, neighbors, colleagues, and friends.

73. As a result of Defendants' failure to prevent the Data Breach, Plaintiff and Class Members have suffered and will continue to suffer injuries, including out of pocket expenses; loss of time and productivity through efforts to ameliorate, mitigate, and deal with the future consequences of the Data Breach; theft of their valuable PII and/or PHI; the imminent and certainly impeding injury flowing from fraud and identity theft posed by their PII/PHI being disclosed to unauthorized recipients and cybercriminals; damages to and diminution in value of their PII and/or PHI; and continued risk to Plaintiff's and the Class Members' PII and/or PHI, which remains in the possession of Defendants and which is subject to further breaches so long as Defendants fail to undertake appropriate and adequate measures to protect the PII/PHI that was entrusted to it.

V.
CLASS ALLEGATIONS

74. Plaintiff brings this class action on behalf of herself and all other individuals who are similarly situated pursuant to Rule 23 of the Nevada Rules of Civil Procedure.

75. Plaintiff seeks to represent a class of persons to be defined as follows:

All individuals in the United States whose PII and/or PHI was compromised in the Data Breach which was announced on or about March 14, 2023 (the "Class").

76. Excluded from the Class are Defendants, its subsidiaries and affiliates, officers and directors, any entity in which Defendants have a controlling interest, the legal representative, heirs, successors, or assigns of any such excluded party, the judicial officer(s) to whom this action is assigned, and the members of their immediate families.

77. This proposed class definition is based on the information available to Plaintiff at this time. Plaintiff may modify the class definition in an amended pleading or when she moves for class certification,

as necessary to account for any newly learned or changed facts as the situation develops and discovery gets underway.

78. **Numerosity:** Plaintiff is informed and believes, and thereon alleges, that there are at minimum, hundreds of members of the Class described above. The exact size of the Class and the identities of the individual members are identifiable through Defendants' records, including but not limited to the files implicated in the Data Breach.

79. **Commonality**: This action involved questions of law and fact common to the Class. Such common questions include but are not limited to:

a. Whether Defendants had a duty to protect the PII/PHI of Plaintiff and Class Members;

b. Whether Defendants were negligent in collecting and storing Plaintiff's and Class Members' PII/PHI, and breached its duties thereby;

c. Whether Plaintiff and Class Members are entitled to damages as a result of Defendants' wrongful conduct; and

d. Whether Plaintiff and Class Members are entitled to restitution as a result of Defendants' wrongful conduct.

80. **Typicality:** Plaintiff's claims are typical of the claims of the members of the Class. The claims of the Plaintiff and members of the Class are based on the same legal theories and arise from the same unlawful and willful conduct. Plaintiff and members of the Class are all patients of Defendants, each having their PII and/or PHI exposed and/or accessed by an unauthorized third party.

81. **Adequacy of Representation:** Plaintiff is an adequate representative of the Class because her interests do not conflict with the interests of the members of the Class. Plaintiff will fairly, adequately, and vigorously represent and protect the interests of the members of the Class and has no interests antagonistic to the members of the Class. In addition, Plaintiff has retained counsel who are competent and experienced in the prosecution of class action litigation. The claims of Plaintiff and the Class Members are substantially identical as explained above.

82. **Superiority:** This class action is appropriate for certification because class proceedings are superior to other available methods for the fair and efficient adjudication of this controversy and joinder of all members of the Class is impracticable. This proposed class action presents fewer management

difficulties than individual litigation, and provides the benefits of single adjudication, economies of scale, and comprehensive supervision by a single court. Class treatment will create economies of time, effort, and expense, and promote uniform decision-making.

83. **Predominance:** Common questions of law and fact predominate over any questions affecting only individual Class Members. Similar or identical violations, business practices, and injuries are involved. Individual questions, if any, pale by comparison, in both quality and quantity, to the numerous common questions that dominate this action. For example, Defendants' liability and the fact of damages is common to Plaintiff and each member of the Class. If Defendants breached their duty to Plaintiff and Class Members, then Plaintiff and each Class member suffered damages by that conduct.

84. **Injunctive Relief:** Defendants have acted and/or refused to act on grounds that apply generally to the Class, making injunctive and/or declaratory relief appropriate with respect to the Class under NRCP 23 (c)(2).

85. **Ascertainability**: Members of the Class are ascertainable. Class membership is defined using objective criteria and Class Members may be readily identified through Defendants' books and records.

VI.
FIRST CAUSE OF ACTION
NEGLIGENCE
(On Behalf of Plaintiff and the Class)

86. Plaintiff restates and realleges all proceeding allegations above as if fully set forth herein.

87. Defendants owed a duty under common law to Plaintiff and Class Members to exercise reasonable care in obtaining, retaining, securing, safeguarding, deleting and protecting their PII and/or PHI in its possession from being compromised, lost, stolen, accessed, and misused by unauthorized persons. More specifically, this duty including, among other things: (a) designing, maintaining, and testing its security systems to ensure that Plaintiff's and Class Members' PII and/or PHI in Defendants' possession was adequately secured and protected; (b) implementing processes that would detect a breach of its security system in a timely manner; (c) timely acting upon warnings and alerts, including those generated by its own security systems, regarding intrusions to its networks; and (d) maintaining data security measures consistent with industry standards.

88. Defendants had a common law duty to prevent foreseeable harm to others. This duty existed because Plaintiff and Class Members were the foreseeable and probable victims of any inadequate security practices on the part of Defendants. By collecting and storing valuable PII/PHI that is routinely targeted by cyber-criminals for unauthorized access, Defendants were obligated to act with reasonable care to protect against these foreseeable threats.

89. Defendants breached the duties owed to Plaintiff and Class Members and thus was negligent. Defendants breached these duties by, among other things, failing to: (a) exercise reasonable care and implement adequate security systems, protocols and practices sufficient to protect the PII and/or PHI of Plaintiff and Class Members; (b) detect the Data Breach while it was ongoing; (c) maintain security systems consistent with industry standards; and (d) disclose that Plaintiff's and Class Members' PII and/or PHI in Defendants' possession had been or was reasonably believed to have been, stolen or compromised.

90. But for Defendants' wrongful and negligent breach of their duties owed to Plaintiff and Class Members, their PII and/or PHI would not have been compromised.

91. As a direct and proximate result of Defendants' negligence, Plaintiff and Class Members have suffered injuries, including:

a. Theft of their PII and/or PHI;

b. Costs associated with requested credit freezes;

c. Costs associated with the detection and prevention of identity theft and unauthorized use of the PII/PHI;

d. Costs associated with purchasing credit monitoring and identity theft protection services;

e. Lowered credit scores resulting from credit inquiries following fraudulent activities;

f. Costs associated with time spent and the loss of productivity from taking time to address and attempt to ameliorate, mitigate, and deal with the actual and future consequences of the Data Breach – including finding fraudulent charges, cancelling and reissuing cards, enrolling in credit monitoring and identity theft protection

services, freezing and unfreezing accounts, and imposing withdrawal and purchase limits on compromised accounts;

g. The imminent and certainly impending injury flowing from potential fraud and identity theft posed by their PII/PHI being placed in the hands of cyber-criminals;

h. Damages to and diminution in value of their PII/PHI entrusted, directly or indirectly, to Defendants with the mutual understanding that Defendants would safeguard Plaintiff's and Class Members data against theft and not allow access and misuse of their data by others; and

i. Continued risk of exposure to hackers and thieves of their PII/PHI, which remains in Defendants' possession and is subject to further breaches so long as Defendants fail to undertake appropriate and adequate measures to protected Plaintiff.

92. As a direct and proximate result of Defendants' negligence, Plaintiff and Class Members are entitled to damages, including compensatory, punitive, and/or nominal damages, damages in an amount in excess of Fifteen Thousand Dollars ($15,000.00).

93. As a further direct and proximate result of Defendants' conduct as set forth herein, Plaintiff has been required to retain the services of an attorney, and as a direct, natural and foreseeable consequence thereof, has been damaged thereby, and is entitled to reasonable attorneys' fees and costs.

VII.
SECOND CAUSE OF ACTION
NEGLIGENCE *PER SE*
(On Behalf of Plaintiff and the Class)

94. Plaintiff restates and realleges all proceeding factual allegations above as if fully set forth herein.

95. Section 5 of the FTC Act prohibits "unfair . . . practices in or affecting commerce" including, as interpreted and enforced by the FTC, the unfair act or practice by institutions such as Defendants for failing to use reasonable measures to protect PII/PHI. Various FTC publications and orders also form the basis of Defendants' duty.

96. Defendants violated Section 5 of the FTC Act by failing to use reasonable measures to protect PII/PHI and not complying with the industry standards. Defendants' conduct was particularly

unreasonable given the nature and amount of PII/PHI it obtained and stored and the foreseeable consequences of a data breach.

97. Plaintiff and Class Members are customers within the class of persons Section 5 of the FTC Act (and similar state statutes) was intended to protect.

98. Moreover, the harm that has occurred is the type of harm that the FTC was intended to guard against.

99. Defendants' violation of Section 5 of the FTC Act constitutes negligence *per se*.

100. Pursuant to HIPAA, 42 U.S.C. § 1302d, *et. seq.*, and its implementing regulations, Defendants had a duty to implement and maintain reasonable and appropriate administrative, technical, and physical safeguards to protect Plaintiff's and the Class members' electronic PHI.

101. Specifically, HIPAA required Defendants to: (a) ensure the confidentiality, integrity, and availability of all electronic PHI they create, receive, maintain, or transmit; (b) identify and protect against reasonably anticipated threats to the security or integrity of the electronic PHI; (c) protect against reasonably anticipated, impermissible uses, or disclosures of the PHI; and (d) ensure compliance by their workforce to satisfy HIPAA's security requirements. 45 CFR § 164.102, *et. seq.*

102. Defendants violated HIPAA by actively disclosing Plaintiff's and the Class Members' electronic PHI; by failing to provide fair, reasonable, or adequate computer systems and data security practices to safeguard Plaintiff's and Class Members' PHI.

103. Plaintiff and the Class Members are patients within the class of persons HIPAA was intended to protect, as they are patients of Defendants.

104. Moreover, the harm that has occurred is the type of harm that HIPAA was intended to guard against.

105. Defendants' violation of HIPAA constitutes negligence *per se*.

106. As a direct and proximate result Defendants' negligence, Plaintiff and Class Members have been injured as described herein and above, and are entitled to damages, including compensatory, punitive, and nominal damages, in an amount in excess of Fifteen Thousand Dollars ($15,000.00).

///

107. As a further direct and proximate result of Defendants' conduct as set forth herein, Plaintiff has been required to retain the services of an attorney, and as a direct, natural and foreseeable consequence thereof, has been damaged thereby, and is entitled to reasonable attorneys' fees and costs.

VIII.
THIRD CAUSE OF ACTION
BREACH OF IMPLIED CONTRACT
(On Behalf of Plaintiff and the Class)

108. Plaintiff restates and realleges all proceeding factual allegations above as if fully set forth herein.

109. Plaintiff and Class Members were required to provide their PII and/or PHI, including their names, addresses, dates of birth, telephone numbers, email addresses, and various forms of identification and medical information to Defendants as a condition of their use of Defendants' services.

110. Plaintiff and Class Members paid money to Defendants in exchange for services, along with Defendants' promise to protect their PII and/or PHI from unauthorized disclosure.

111. Plaintiff is informed and believes that in their written privacy policies, Defendants expressly promised Plaintiff and Class Members that they would only disclose PII and/or under certain circumstances, none of which relate to the Data Breach.

112. Defendants promised to comply with industry standards and to make sure that Plaintiff's and Class Members' PII and/or would remain protected.

113. Implicit in the agreement between Plaintiff and Class Members and Defendants to provide protected health information and other PII and/or PHI, was the latter's obligation to: (a) use such PII and/or PHI for business purposes only, (b) take reasonable steps to safeguard that PII and/or PHI, (c) to prevent unauthorized disclosures of the PII and/or PHI, (d) to provide Plaintiff and Class Members with prompt and sufficient notice of any and all unauthorized access and/or theft of their PII and/or PHI, (e) to reasonably safeguard and protect the PII and/or PHI of Plaintiff and Class Members from unauthorized disclosure or uses, (f) to retain the PII and/or PHI only under conditions that kept such information secure and confidential.

114. Without such implied contracts, Plaintiff and Class Members would not have provided their PII and/or PHI to Defendant.

115. Plaintiff and Class Members fully performed their obligations under the implied contract with Defendants, however, Defendants did not.

116. Defendants breached the implied contracts with Plaintiff and Class Members by failing to reasonably safeguard and protect Plaintiff and Class Members' PII and/or, which was compromised as a result of the Data Breach.

117. As a direct and proximate result of Defendants breach of implied contract, Plaintiff and Class Members have been injured as described herein and above, and are entitled to damages, including compensatory, punitive, and nominal damages, in an amount in excess of Fifteen Thousand Dollars ($15,000.00).

118. As a further direct and proximate result of Defendants' conduct as set forth herein, Plaintiff has been required to retain the services of an attorney, and as a direct, natural and foreseeable consequence thereof, has been damaged thereby, and is entitled to reasonable attorneys' fees and costs.

IX.
FOURTH CAUSE OF ACTION
UNJUST ENRICHMENT
(On Behalf of Plaintiff and the Class)

119. Plaintiff restates and realleges all proceeding factual allegations above as if fully set forth herein.

120. Plaintiff and Class Members conferred a monetary benefit on Defendants. Specifically, they purchased goods and services from Defendants and in so doing provided Defendants with their PII and/or PHI. In exchange, Plaintiff and Class Members should have received from Defendants the goods and services that were the subject of the transaction and have their PII and/or PHI protected with adequate data security.

121. Defendants knew that Plaintiff and Class Members conferred a benefit which Defendants accepted. Defendants profited from these transactions and used the PII and/or PHI of Plaintiff and Class Members for business purposes.

122. The amounts Plaintiff and Class Members paid for goods and services were used, in part, to pay for use of Defendants' network and the administrative costs of data management and security.

123. Under the principles of equity and good conscience, Defendants should not be permitted to retain the money belonging to Plaintiff and Class Members, because Defendants failed to implement appropriate data management and security measures that are mandated by industry standards.

124. Defendants failed to secure Plaintiff's and Class Members' PII and/or PHI and, therefore, did not provide full compensation for the benefit Plaintiff and Class Members provided.

125. Defendants acquired the PII and/or through inequitable means in that it failed to disclose the inadequate security practices previously alleged.

126. If Plaintiff and Class Members knew that Defendants had not secured their PII and/or PHI, they would not have agreed to Defendants' services.

127. Plaintiff and Class Members have no adequate remedy at law.

128. As a direct and proximate result of Defendants' conduct, Plaintiff and Class Members have suffered and will suffer injury, including but not limited to: (i) actual identity theft; (ii) the loss of the opportunity how their PII and/or PHI is used; (iii) the compromise, publication, and/or theft of their PII and/or PHI; (iv) out-of-pocket expenses associated with the prevention, detection, and recovery from identity theft, and/or unauthorized use of their PII and/or PHI; (v) lost opportunity costs associated with effort expended and the loss of productivity addressing and attempting to mitigate the actual and future consequences of the Data Breach, including but not limited to efforts spent researching how to prevent, detect, contest, and recover from identity theft; (vi) the continued risk to their PII and/or PHI, which remain in Defendants' possession and is subject to further unauthorized disclosures so long as Defendants fail to undertake appropriate and adequate measures to protect PII and/or PHI in their continued possession; and (vii) future costs in terms of time, effort, and money that will be expended to prevent, detect, contest, and repair the impact of the PII and/or compromised as a result of the Data Breach for the remainder of the lives of Plaintiff and Class Members.

129. As a direct and proximate result of Defendants' conduct, Plaintiff and Class Members have suffered and will continue to suffer other forms of injury and/or harm.

130. Defendants should be compelled to disgorge into a common fund or constructive trust, for the benefit of Plaintiff and Class Members, proceeds that they unjustly received from them. In the

alternative, Defendants should be compelled to refund the amounts that Plaintiff and Class Members overpaid for Defendants' services.

131. As a further direct and proximate result of Defendants' conduct as set forth herein, Plaintiff has been required to retain the services of an attorney, and as a direct, natural and foreseeable consequence thereof, has been damaged thereby, and is entitled to reasonable attorneys' fees and costs.

X.
FIFTH CAUSE OF ACTION
BREACH OF CONFIDENCE – PUBLIC DISCLOSURE OF PRIVATE FACTS
(On Behalf of Plaintiff and the Class)

132. Plaintiff restates and realleges all proceeding factual allegations above as if fully set forth herein.

133. Plaintiff and Class Members were required to provide their PII and/or PHI to Defendants as a condition of their use of Defendants' services.

134. Plaintiff and Class Members paid money to Defendants in exchange for services, along with Defendants' promise to protect their PII and/or PHI from unauthorized disclosure.

135. Plaintiff is informed and believes that in their written privacy policies, Defendants expressly promised Plaintiff and Class Members that it would only disclose PII and/or PHI under certain circumstances, none of which relate to the Data Breach.

136. Implicit in the agreement between Plaintiff and Class Members and Defendants to provide PII and/or PHI, was the latter's obligation to: (a) use such PII and/or PHI for business purposes only, (b) take reasonable steps to safeguard that PII and/or PHI, (c) prevent unauthorized disclosures of the PII and/or PHI, (d) provide Plaintiff and Class Members with prompt and sufficient notice of any and all unauthorized access and/or theft of their PII and/or PHI, (e) reasonably safeguard and protect the PII and/or PHI of Plaintiff and Class Members from unauthorized disclosure or uses, (f) retain the PII and/or PHI only under conditions that kept such information secure and confidential.

137. Without such implied contracts, Plaintiff and Class Members would not have provided their PII and/or to Defendant.

138. Plaintiff and Class Members fully performed their obligations under the implied contract with Defendants, however, Defendants did not.

139. Defendants breached the implied contracts with Plaintiff and Class Members by failing to reasonably safeguard and protect Plaintiff and Class Members' PII and/or PHI, which was compromised as a result of the Data Breach.

140. Plaintiff and Class Members' PII and/or PHI was compromised and made public as a result of the Data Breach, which was offensive and objectionable to a reasonable person with ordinary sensibilities.

141. As a direct and proximate result of Defendants' conduct, Plaintiff and Class Members have been injured as described herein and above, and are entitled to damages, including compensatory, punitive, and nominal damages, in an amount in excess of Fifteen Thousand Dollars ($15,000.00).

142. As a further direct and proximate result of Defendants' conduct as set forth herein, Plaintiff has been required to retain the services of an attorney, and as a direct, natural and foreseeable consequence thereof, has been damaged thereby, and is entitled to reasonable attorneys' fees and costs.

XI.
SIXTH CAUSE OF ACTION
VIOLATION OF NEVADA'S CONSUMER FRAUD ACT Nevada Revised Statutes 41.600
(On Behalf of Plaintiff and the Class)

143. Plaintiff restates and realleges all proceeding factual allegations above as if fully set forth herein.

144. Defendants engaged in unfair and unlawful acts and practices by failing to maintain adequate procedures to avoid a data breach, and permitting access to consumer reports by data thieves, for whom Defendants had no reasonable grounds to believe would be used for a proper purpose. Plaintiff and Class members relied on Defendants' implied promise of data security when providing their PII and/or PHI to Defendants.

145. Defendants conduct violated NRS 598.0917(7) because it constituted a tender of "goods advertised for sale . . . or tendering terms of sale or lease less favorable than the terms advertised," i.e., goods offered for sale by credit card without the corresponding promise that a consumer's PII and/or PHI would be kept reasonably safe from harm.

146. Defendants' violations of NRS 598.0917(7) constituted "consumer fraud" for purposes of NRS 41.600(2)(e).

147. Defendants also breached its duty under NRS 603A.210, which requires any data collector "that maintains records which contain personal information" of Nevada residents to "implement and maintain reasonable security measures to protect those records from unauthorized access, acquisition, . . . use, modification or disclosure." Defendants did not take such reasonable security measures, as shown by a system-wide breach of payment processing systems.

148. Defendants also breached its duty under NRS 603A.215, which requires any data collector doing business in Nevada who accept payment cards in connection with a sale of goods or services to "comply with the current version of the . . . PCI Security Standards Council . . . with respect to those transactions." On information and belief, Defendants failed to adhere to PCI standards, and was grossly negligent because the violation occurred in multiple stores across the United States.

149. Defendants' violations of NRS 598.0923(3) constituted "consumer fraud" for purposes of NRS 41.600(2)(e).

150. Additionally, NRS 598.0923(3) provides that a violation of any federal or Nevada law constitutes consumer fraud. Thus, Defendants' violations of the FTC Act, NRS 598.0917(7), and NRS 603A violated NRS 598.0923(3).

151. Defendants' violations of NRS 598.0923(3), NRS 598.0917(7), and NRS 603A in turn constituted "consumer fraud" for purposes of NRS 41.600(2)(e).

152. Defendants engaged in an unfair practice by engaging in conduct that is contrary to public policy, unscrupulous, and caused injury to Plaintiff and Class Members.

153. As a direct and proximate result of the foregoing, Plaintiff and Class Members have suffered injuries including, but not limited to actual damages, and in being denied a benefit conferred on them by the Nevada legislature.

154. As a result of these violations, Plaintiff and Class Members are entitled to an award of actual damages in excess of of Fifteen Thousand Dollars ($15,000.00), equitable injunctive relief preventing Defendants to continue to violate the PCI DSS standards, as well as an award of reasonable attorney's fees and costs.

///

///

PRAYER FOR RELIEF

WHEREFORE, Plaintiff, on behalf of herself and all others similarly situated, respectfully requests the following relief:

1. An Order certifying this case as a class action;
2. An Order appointing Plaintiff as the class representative;
3. An Order appointing undersigned counsel as class counsel;
4. A mandatory injunction directing Defendants to hereinafter adequately safeguard the PII and/or PHI of the Class by implementing improved security procedures and measures;
5. For economic damages in an amount in excess of Fifteen Thousand Dollars ($15,000.00). An award of costs and expenses;
6. For special damages according to proof;
7. An award of attorneys' fees and costs;
8. Prejudgment interest; and
9. For such other further relief as the Court may deem just and proper.

DATED this 30th day of March 2023.

THE BOURASSA LAW GROUP

By: */s/ Jennifer A. Fornetti*

MARK J. BOURASSA, ESQ. (NBN 7999)
JENNIFER A. FORNETTI, ESQ. (NBN 7644)
VALERIE S. GRAY, ESQ. (NBN 14716)
2350 W. Charleston Blvd., Suite 100
Las Vegas, Nevada 89102

GARY F. LYNCH (*pro hac vice* forthcoming)
NICHOLAS A. COLELLA (*pro hac vice* forthcoming)
PATRICK D. DONATHEN (*pro hac vice* forthcoming)
LYNCH CARPENTER LLP
1133 Penn Avenue, 5th Floor
Pittsburgh, PA 15222

Attorneys for Plaintiff

DEMAND FOR JURY TRIAL

Plaintiff, by and through their attorneys of record, The Bourassa Law Group hereby demands a jury trial of all of the issues in the above matter.

DATED this 30th day of March 2023.

THE BOURASSA LAW GROUP

By: */s/ Jennifer A. Fornetti*

MARK J. BOURASSA, ESQ. (NBN 7999)
JENNIFER A. FORNETTI, ESQ. (NBN 7644)
VALERIE S. GRAY, ESQ. (NBN 14716)
2350 W. Charleston Blvd., Suite 100
Las Vegas, Nevada 89102

GARY F. LYNCH (*pro hac vice* forthcoming)
NICHOLAS A. COLELLA (*pro hac vice* forthcoming)
PATRICK D. DONATHEN (*pro hac vice* forthcoming)
LYNCH CARPENTER LLP
1133 Penn Avenue, 5th Floor
Pittsburgh, PA 15222

Attorneys for Plaintiff